WILKINSON) BARKER) KNAUER) LLP

2300 N STREET, NW
SUITE 700
WASHINGTON, DC 20037
TEL 202.783.4141
FAX 202.783.5851
www.wbklaw.com

March 1, 2013

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, S.W.
Room TW-A325
Washington, DC 20554

Re: Buffalo-Lake Erie Wireless Systems Co., LLC d/b/a Blue Wireless
Certification of CPNI Filing – Calendar Year 2012
EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to 47 C.F.R. § 64.2009(e), attached is the calendar-year 2012 CPNI certification filing for Buffalo-Lake Erie Wireless Systems Co., LLC d/b/a Blue Wireless (FRN 0009403692). Please contact the undersigned if there are any questions concerning this submission.

Sincerely yours,

WILKINSON BARKER KNAUER, LLP

By: _____
Lawrence J. Movshin

Encl.

ANNUAL SECTION 64.2009(E) CERTIFICATION
EB Docket No. 06-36

Annual § 64.2009(e) CPNI Certification Covering the Prior Calendar Year 2012
Date Filed: March 1, 2013
Company: Buffalo-Lake Erie Wireless Systems Co., LLC (*d/b/a* Blue Wireless)
Form 499 Filer ID Number: 824700
Name of Signatory: Brian Gelfand
Title of Signatory: Vice President

I, Brian Gelfand, certify that I am a duly authorized officer of **Buffalo-Lake Erie Wireless Systems Co., LLC** ("Blue Wireless") and, acting as an agent of Blue Wireless, that I have personal knowledge that Blue Wireless has established operating procedures that are adequate to ensure compliance with the Customer Proprietary Network Information ("CPNI") rules of the Federal Communications Commission ("Commission"), codified at 47 C.F.R. Part 64 Subpart U, implementing Section 222 of the Communications Act of 1934, as amended.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in sections 64.2001 *et seq*. of the Commission's rules.

Blue Wireless has not taken any actions against data brokers in the past year and has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Brian Gelfand

STATEMENT REGARDING OPERATING PROCEDURES
IMPLEMENTING 47 C.F.R. PART 64 SUBPART U
GOVERNING USE OF
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)
March 1, 2013

The following statement explains how the operating procedures of **Buffalo-Lake Erie Wireless Systems Co., LLC ("Blue Wireless")** ensure that it is in compliance with the Commission's CPNI rules, as codified at 47 C.F.R. Part 64 Subpart U and is relevant to calendar year 2012.

I. Use of customer proprietary network information without customer approval.

A. Blue Wireless may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service to which the customer already subscribes from Blue Wireless without customer approval.

B. Blue Wireless may not use, disclose, or permit access to CPNI to market to a customer service offerings that are within a category of service to which the subscriber does not already subscribe from Blue Wireless. Blue Wireless unless Blue Wireless has customer approval to do so, except as described in Section I.C.

(1) Blue Wireless may use, disclose or permit access to CPNI derived from their provision of local exchange service or interexchange service, without customer approval, for the provision of CPE and information services, such as call answering, voice mail or messaging, voice storage and retrieval services, and fax storage and retrieval services.

(2) Blue Wireless may not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

C. Blue Wireless may use, disclose, or permit access to CPNI, without customer approval, as follows:

(1) Blue Wireless may use, disclose, or permit access to CPNI, in its provision of inside wiring installation, maintenance, and repair services.

(2) Blue Wireless may use, disclose, or permit access to CPNI for the purpose of conducting research on the health effects of commercial mobile radio services ("CMRS").

(3) Blue Wireless may use CPNI to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain Centrex features.

D. Blue Wireless may use, disclose, or permit access to CPNI to protect Blue Wireless's rights or property; to protect its users and other carriers from fraudulent, abusive, or

unlawful use of, or subscription to, Blue Wireless's services; and to render, provision, bill or collect for services.

Blue Wireless presently offers CMRS to its customers. Blue Wireless has not engaged in, and has no present plans to engage in the use of, disclosure of or permitting access to CPNI for marketing purposes. Nor does Blue Wireless have any plans to engage in any marketing or cross marketing that would require either opt-in or opt-out customer approval to use, disclose or permit access to CPNI under Sections 64.2007 and 64.2008 of the Commission's rules. If, in the future, Blue Wireless should determine that it will engage in any marketing or cross marketing not allowed by Section 64.2005 or Section 222 of the Communications Act without customer approval, Blue Wireless will develop and implement the appropriate operating procedures to ensure compliance with the opt-in and opt-out notice, approval, recordkeeping and other relevant requirements of the FCC's rules.

II. Safeguards required for use and disclosure of customer proprietary network information.

A. Blue Wireless must implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

B. Blue Wireless may release call detail information during a customer initiated telephone contact only if reasonable authentication procedures are complied with and (1) the customer provides Blue Wireless with a pre-established password, (2) Blue Wireless, at the customer's request, sends the call detail information to the customer's address of record provided the address of record has been associated with the account for at least thirty (30) days, or (3) Blue Wireless calls the telephone number of record to disclose the call detail information. Blue Wireless is permitted to create a back-up customer authentication method for lost or forgotten passwords. Blue Wireless is also prohibited from releasing call detail information during a retail visit without the appropriate password or valid photo identification.

However, if the during a customer-initiated telephone contact, the customer is able to provide without assistance from Blue Wireless personnel all of the call detail information necessary to address a customer service issue (i.e., the telephone number called, when it was called, and if applicable the amount charged for the call), then Blue Wireless personnel are permitted to proceed with its routine customer care procedures.

C. Blue Wireless must authenticate a customer without readily available biographical or account information prior to allowing the customer on-line access to CPNI related telecommunication service account. Once authenticated, the customer may only obtain on-line access to CPNI related telecommunications service account through a password.

D. Blue Wireless is required to notify customers immediately when a password or back-up means of authentication for lost or forgotten passwords, on-line account, or address of record is created or changed. Such notification is not required when the customer initiates service, including the selection of a password.

E. Business customers are exempt from the password requirements if, the customer is contractually bound to Blue Wireless, is serviced by a dedicated Blue Wireless account representative as the primary contact, and within the contract Blue Wireless is responsible to address its CPNI obligations. If, at any point, the business customer must go through a call center to reach a customer service representative, then the exemption does not apply.

F. Blue Wireless must train its personnel as to when they are and are not authorized to use CPNI, and Blue Wireless must have an express disciplinary process in place.

Blue Wireless's personnel are trained on the appropriate uses of CPNI, and Blue Wireless has internal procedures in place to protect against the unauthorized disclosure of CPNI to third parties. Blue Wireless has an express disciplinary process in place that addresses non-compliance with Blue Wireless policies, including those relating to CPNI.

G. Blue Wireless must maintain a record, electronically or in some other manner, of its own and its affiliates' sales and marketing campaigns that use its customers' CPNI. Blue Wireless shall maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record must include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. Blue Wireless shall retain the record for a minimum of one year.

H. Blue Wireless must establish a supervisory review process regarding its compliance with the FCC's CPNI rules for outbound marketing situations and maintain records of its compliance for a minimum period of one year. Specifically, sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.

I. Blue Wireless must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI, which may include encryption of its databases. Blue Wireless must properly authenticate a customer prior to disclosing CPNI based on a customer-initiated telephone contact, on-line account access, or an in-store visit.

Blue Wireless must take measures to protect CPNI stored in its internal databases from potential unauthorized access, and evaluate and increase its security measures should it discover an increase in attempts to gain access to unauthorized information.

J. Blue Wireless must provide written notice within five business days to the FCC of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

(1) The notice shall be in the form of a letter, and shall include Blue Wireless's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information.

(2) Such notice must be submitted even if Blue Wireless offers other methods by which consumers may opt-out.

K. Blue Wireless has a general duty to first inform federal law enforcement agencies, followed up by notification to affected customers, after reasonable determination of a breach of its customers' CPNI.

(1) Blue Wireless must file an electronic notification to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) within seven (7) business days through the central reporting facility furnished by the Commission.

(2) Blue Wireless is prohibited from notifying customers or the general public of the breach until seven (7) business days have passed after notification to the USSS and FBI unless under certain specified circumstances: (a) Blue Wireless identifies an "extraordinary need to notify customers" before that period or (b) an ongoing or potential investigation or national security requires customer disclosure to be potentially delayed for up to thirty (30) days. Blue Wireless must notify the affected customer(s) after the applicable period.

(3) Blue Wireless must maintain a record, whether electronically or in some other manner of any breaches discovered, notifications made to the USSS or FBI and notifications made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Records must be maintained for a two (2) year period.

Blue Wireless has implemented operating procedures to comply with all of the above requirements. In particular, Blue Wireless notes the following:

Record-Keeping. Blue Wireless maintains records of any sales and marketing campaigns that use CPNI. Such records include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as part of the campaign. Blue Wireless will retain these records for one year. As noted, to date Blue Wireless has not used CPNI for marketing purposes.

Supervisory Review. All outbound marketing is done pursuant to supervisory review and approval. Failure to comply with the company's policies may result in disciplinary action, up to and including termination of employment. Employees are trained as to permitted and prohibited use of CPNI.

Reporting. As noted above, Blue Wireless does not currently engage in marketing that requires customer approval regarding CPNI. To the extent Blue Wireless changes its policies in the future in a manner that opt-out approval is required, Blue Wireless will provide the FCC with written notice within five business days of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt out is more than an anomaly.

Safeguards. Blue Wireless has implemented reasonable measures to protect CPNI from unauthorized access, such as pretexting, including compliance with the customer authentication safeguard requirements of the FCC's rules. Blue Wireless requires customers to provide account specific password information or present photo identification before

reviewing any customer account information. Blue Wireless does not provide call detail information to customers under any circumstances. Further, company databases are restricted from public access and only authorized representatives of the company are given passwords to access the database to be used only in association with their job description. Blue Wireless notifies customers of account changes in accordance with FCC rules.

<u>Breach Notification</u>. Blue Wireless monitors the protection of CPNI and records any breaches or discoveries that would suspect a breach. Blue Wireless has policies in place to report any breach to law enforcement and customers in accordance with FCC rules, and to maintain records of any such breach(es) for at least two years. At this point in time, no such breaches or discoveries have occurred.

V. Supplemental Information

The FCC's rules require that the annual certification filed pursuant to 47 C.F.R. § 64.2009(e) disclose any actions taken against data brokers and a summary of all consumer complaints received in the previous calendar year regarding the unauthorized release of CPNI.

Blue Wireless has taken no action against data brokers during the prior calendar year, and received no consumer complaints relating to CPNI in that period. Blue Wireless has no information regarding pretexters' processes for attempting to access CPNI and steps taken to protect CPNI from pretexters beyond what the FCC has been informed of already.